UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,167	09/14/2000	Anton Enterrottacher	P00.0637	5982

24573 7590 10/19/2004

BELL, BOYD & LLOYD, LLC
PO BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/646,167	ENTERROTTACHER ET AL.
	Examiner	Art Unit
	Zachary A Davis	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 02 June 2004. Claims 4-7 have been amended. New Claims 8-12 have been added. Claims 4-12 are pending in the present application.

Priority

2. It is noted that Applicant has amended the specification to include a reference to prior Application No. PCT/DE99/00415, filed 16 February 1999.

Response to Arguments

3. Applicant's arguments with respect to claims 4-7 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. The objection to Claim 7 for informalities has been withdrawn in view of the amendment to the Claim.

5. Claim 9 is objected to because of the following informalities: the mathematical equation at line 5 of the claim includes a variable "sD"; it appears that this is intended to refer to "sAD", the secret key of the administrator. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 4-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of the claims raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. Specifically, the claims are directed to a method of authenticating key devices. However, the claims do not provide any specific positive method steps that would achieve such an authentication, only steps of "assigning".

8. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the statutory classes of invention.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 4-6, 8, and 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Mittra, US Patent 5748736.

In reference to Claim 4, Mittra discloses a method for authenticating key devices, in which each key device is assigned a device-specific certificate (column 11, lines 35-38), including the steps of assigning each device a group-specific public key (column 8, lines 15-35) and assigning each key device a group-specific signature of its certificate (column 11, lines 35-41).

In reference to Claim 5, Mittra further discloses that the public key and signature are allocated during a first initialization (column 8, lines 33-35).

In reference to Claim 6, Mittra further discloses that each key device is compared with a stored list of approved key devices (column 7, lines 52-57).

In reference to Claim 8, Mittra discloses a method for authenticating key devices, in which each key device is assigned a device-specific certificate (column 11, lines 35-

38), including the steps of assigning each device a group-specific public key (column 8, lines 15-35), assigning each key device a group-specific signature of its certificate (column 11, lines 35-41), establishing a link between at least two key devices and transmitting a certificate and signature from one of the key devices to another of the key devices (column 11, lines 35-41, where the signed certificates are sent along with any message sent to the group).

In reference to Claim 12, Mittra further discloses that each key device is compared with a stored list of approved key devices (column 7, lines 52-57).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 7 and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra in view of Schneier, *Applied Cryptography*.

In reference to Claim 7, Mittra discloses everything as applied to Claim 4 above. Mittra further discloses establishing a link between at least two key devices and transmitting a certificate and signature from one of the key devices to another of the key devices (column 11, lines 35-41, where the signed certificates are sent along with any message sent to the group). Mittra also discloses that communications must include a

signature in order to verify the message (column 7, lines 60-63); however, Mittra does not explicitly disclose the relationship used to verify the signature.

Schneier discloses that public key cryptography can be used for digitally signing documents. Specifically, a signature is formed by encrypting a document with the sender's private key, and the signature is verified by the receiver by decrypting the document with the sender's public key (page 37, "Signing Documents with Public-Key Cryptography").

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification taught by Schneier in the authentication method of Mittra, in order to allow the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37).

In reference to Claim 9; Mittra discloses everything as applied to Claim 8 above. Mittra also discloses that communications must include a signature in order to verify the message (column 7, lines 60-63); however, Mittra does not explicitly disclose the relationship used to verify the signature. Schneier discloses that public key cryptography can be used for digitally signing documents. Specifically, a signature is formed by encrypting a document with the sender's private key, and the signature is verified by the receiver by decrypting the document with the sender's public key (page 37, "Signing Documents with Public-Key Cryptography"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification taught by Schneier in the authentication method of Mittra, in order to

allow the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37).

In reference to Claim 10, Mittra discloses a method for authenticating key devices, in which each key device is assigned a device-specific certificate (column 11, lines 35-38), including the steps of assigning each device a group-specific public key (column 8, lines 15-35), assigning each key device a group-specific signature of its certificate (column 11, lines 35-41), establishing a link between at least two key devices and transmitting a certificate and signature from one of the key devices to another of the key devices (column 11, lines 35-41, where the signed certificates are sent along with any message sent to the group). Mittra also discloses that communications must include a signature in order to verify the message (column 7, lines 60-63); however, Mittra does not explicitly disclose the relationship used to verify the signature.

Schneier discloses that public key cryptography can be used for digitally signing documents. Specifically, a signature is formed by encrypting a document with the sender's private key, and the signature is verified by the receiver by decrypting the document with the sender's public key (page 37, "Signing Documents with Public-Key Cryptography").

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification taught by Schneier in the authentication method of Mittra, in order to allow the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37).

In reference to Claim 11, Mittra further discloses that the public key and signature are allocated during a first initialization (column 8, lines 33-35).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Gasser et al, US Patent 5220604, disclose a method in which devices are authenticated, using signed certificates, based on groups to which the devices belong.

b. Carroni et al, US Patent 6049878, disclose a system for sending information privately to members of a group in which the group members are authenticated. Carroni et al, US Patent 5822434, further disclose the use of certificates for authentication and identification of devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870, as of 26 October 2004. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137